**DATE(S) ISSUED:**
05/14/2013

**SUBJECT:**
Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (MS13-042)

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Microsoft Publisher which could allow an attacker to take complete control of an affected system. Microsoft Publisher, a component of Microsoft Office, is an application that allows users to create marketing materials and other types of publications. Exploitation may occur if a user opens a specially crafted Publisher file. This file may be received as an email attachment, or downloaded via the Web. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**SYSTEMS AFFECTED:**
· Microsoft Office 2010 SP1 (32-bit)
· Microsoft Office 2010 SP1 (64-bit)
· Microsoft Office 2007 SP3
· Microsoft Office 2003 SP3

**RISK:**

**Government:**
· Large and medium government entities: **High**
· Small government entities: **High**

**Businesses:**
· Large and medium business entities: **High**
· Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Eleven vulnerabilities have been discovered in Microsoft Publisher, which could allow an attacker to take complete control of an affected system. These vulnerabilities may be exploited if a user visits, or is redirected to a web page; or opens a malicious file that was designed to take advantage of these vulnerabilities. These vulnerabilities may also be exploited if a user opens an email that has a specially crafted file designed to leverage these vulnerabilities. All of these vulnerabilities are caused by the same underlying problem, which is Microsoft Publisher failing to properly handle values in memory when parsing Publisher files.

Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**
The following actions should be taken:
· Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
· Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
· Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
· Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

**REFERENCES:**

**Microsoft:**
https://technet.microsoft.com/en-us/security/bulletin/ms13-042

**CVE:**
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1316
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1317
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1318
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1319
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1320
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1321
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1322
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1323

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1327
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1328
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1329